**HTTP hay HTTPS? Đâu sẽ là lựa chọn tối ưu?**

**Thử nghiệm:**

Đầu tiên hãy thử nghiệm bắt gói tin http bằng Wireshark ở hai trang web iuh.edu.vn và uit.edu.vn

Đây là kết quả thử nghiệm khi bắt gói tin từ trang web iuh.edu.vn:

Graphical user interface, application

Description automatically generated

Đây là kết quả thử nghiệm khi bắt gói tin từ trang web uit.edu.vn:

Graphical user interface, application

Description automatically generated

**Nhận xét:**

Khi ta thực hiện việc bắt gói tin ở trang web iuh.edu.vn ta dễ dàng bắt được gói tin http nhưng ở phía của trang uit.edu.vn ta không làm được điều đó. Vậy nguyên nhân là do đâu?

Sau quá trình tìm hiểu, thấy được ở trang uit.edu.vn đã sử dụng internet protocol là https còn phía của trang web iuh.edu.vn chỉ sử dụng http.

**Nghiên cứu 1:**

Như đã biết, HTTP được viết tắt của cụm từ HyperText Transfer Protocol và cụm từ HTTPS cũng vậy nhưng có thêm từ S cuối đại diện cho chữ Secure.

Vậy yếu tố Secure trong HTTPS được thể hiện như thế nào? Đó là việc mã hóa bằng TSL hoặc SSL của giao thức HTTPS.

Bằng cách sử dụng những cơ chế mã hóa đặc biệt với các bộ mã giúp cho những gói tin được mã hóa trước khi gửi đi, gửi về, đảm bảo được việc tránh khỏi những kẻ nghe lén và cuộc tấn công từ bên thứ ba, đảm bảo được tín bảo mật.

*Nhận biết:*

Khi trang web sử dụng HTTPS, sẽ có dấu hiệu ở phần Secure (góc phải phía bên trái của màng hình):

Graphical user interface, text, application, chat or text message

Description automatically generated

Khi ấy ta sẽ thấy chứng nhận và phần Issued by sẽ có thông tin RapidSSL TLS …

Còn ở trang web chỉ sử dụng HTTP:

Graphical user interface, text

Description automatically generated

Sẽ không thấy được chứng nhận đó.

**Nghiên cứu 2:**

Nhưng trên thực tế cũng sẽ có những công cụ để có thể bắt gói tin khi trang web đó sử dụng HTTPS, ví dụ đó là công cụ sslstrip được sử dụng trên nền tảng của Kali Linux:

Bằng cách sử dụng đón gói tin https từ router và chuyển đổi thành http bên thứ 3 dễ dàng tấn công và đánh cắp dữ liệu

Máy A https Router http Trang web

https http

Bên thứ 3

chuyển đổi https thành http bằng công cụ sslstrip

Khi thực hiện cách này cần phải có Interface của máy tấn công ví dụ wlan1, lo, eth1, eth0. Thứ 2 đó là Ngõ IP của máy tấn công ví dụ 192.168.0.1 và IP của mục tiêu ví dụ 192.168.0.7

Khi đó ta có thể thực hiện đón gói tin và khai thác những thông tin như tài khoản mật khẩu của trang web truy cập ví dụ như mạng xã hội facebook, hay các website của các ngân hàng, các website của các sàn thương mại điện tử…

**Nghiên cứu 3:**

Ngoài ra còn có thể thiết lập lại môi trường trên wireshark để có thể đóng và giải mã gói tin SSL nhằm khai thác thông tin. Hoặc có thể sử dụng thêm công cụ sslsplit được cài sẵn trên Kali Linux để khai thác gói tin sslsplit.

**Kết luận:**

Qua đó thấy được rằng là dù được sử dụng HTTPS nhưng vẫn có được một số rủi ro nhất định, do đó các chuyên gia bảo mật phải không ngừng nâng cao tính an toàn của hệ thống mà mình đang quản lý.